



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/240,265	01/29/1999	MARK E. PETERS	CR9-98-095	7166

25259 7590 06/05/2002

IBM CORPORATION  
3039 CORNWALLIS RD.  
DEPT. T81 / B503, PO BOX 12195  
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER

MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 06/05/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/240,265

Applicant(s)

PETERS, MARK E.

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 11 March 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-3 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the request for reconsideration filed 11 March 2002.

### ***Response to Arguments***

2. Applicant's arguments with respect to claims 1-3 have been considered but are moot in view of the new ground(s) of rejection.

### ***Drawings***

3. Figures 1 and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (5923756) in view of Schneier (*Applied Cryptography*).

In lines 32-35 of column 10, Shambroom discusses a certificate that supports one or more cryptographic algorithms. The certificate can resemble an X.509 certificate. Shambroom does not say exactly what would be included in this certificate if

it were to resemble an X.509 certificate. On pages 574 and 575, Schneier describes the X.509 certificate. As can be seen in figure 24.2, the certificate includes a section that identifies the algorithm, parameters, and a public key. There is also a section for a signature. These read on the first clause of applicant's first claim. To be incorporated with Shambroom's teachings while maintaining the look of an X.509 certificate, there would be a section that identified the alternate algorithm and provided a key. There would also be a signature to authenticate this key. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made that the X.509 certificate that supports multiple cryptographic algorithms in Shambroom would include sections identifying the second algorithm and its key as well as a signature for authenticating that second key.

With respect to claim 2, pages 480 and 481 of Schneier discuss elliptic curve public key systems. RSA is first mentioned on page 17. According to Schneier, it is the most popular public-key algorithm. There are trade-offs between the two, particularly in terms of the relative computational workloads of the two entities (signer and verifier). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to support RSA and an elliptic curve cryptosystem with the X.509 certificate taught by Shambroom.

Both signatures verify at least part of the certificate and hence read on claim 3.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703)

Art Unit: 2132

305-1338. The examiner can normally be reached on between 9 AM and 6 PM,  
Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

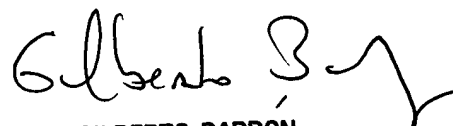
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



DJM

May 31, 2002

Douglas J. Meislahn  
Examiner  
Art Unit 2132



GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100